APHIS DIRECTIVE 1650.2 8/18/93

SECURITY IN AGENCY-OCCUPIED FIELD OFFICES

1. PURPOSE

This Directive prescribes procedures for protecting Agency-occupied buildings or space and for reporting thefts or other unlawful acts which occur in, or on the grounds of, Agency-occupied buildings at field locations.

2. SECURITY MEASURES

The procedures contained in this Directive implement security requirements established by the General Services Administration (GSA), the U.S. Department of Agriculture (USDA), and/or the Agency to protect Government premises and employees.

a. Establishment of Security Measures.

(1) Federal Buildings and Space Leased by GSA. The local Federal Protective Service prescribes appropriate security measures at these locations. Employees and non-Government persons must follow whatever procedures are required for entering and exiting the buildings.

(2) Agency-Controlled Buildings Which Are Government Owned. The highest ranking Agency official (such as the Regional Director, Area Director, or Officer-in-Charge) is known as the Designated Official and is responsible for establishing security procedures to ensure that Government property and employees are protected. Employees and non-Government persons must follow the established procedures.

(3) Agency-Occupied Offices in Agency-Leased Space. The lessor may prescribe security procedures for protecting the space. Program officials are responsible for ensuring that security measures are established for protection items within Agency-occupied space.

b. Identification Cards. All employees must have valid USDA, Agency, or program identification (ID) cards. These are issued to identify persons who are authorized admittance to conduct official business. Employees who do not have ID cards should contact their supervisors.

c. Access to Agency-Occupied Space.

(1) Employees must carry and be prepared to display

their USDA or program ID card if requested to do so.

(2) Non-Government persons should contact program officials and/or the building owner, lessor, or manager (as appropriate) to gain access to space. Program officials should make special arrangements for access after normal work hours of the locations.

(3) Persons who refuse to show identification may be denied entry into Agency-occupied space.

(4) Security guards or Agency officials may inspect items which could be carrying concealed property or dangerous materials. Persons who refuse to allow search and inspection of materials may be denied entry into the building or Agency-occupied space.

d. Locked Rooms. Some offices may need to be locked to protect Government property from theft or damage. Program officials should arrange to have locks installed or keys made where needed and establish procedures to ensure the control and return of keys when no longer needed.

3. SECURITY OF AUTOMATED EQUIPMENT

Physical security requirements for Federal Information Processing (FIP) equipment should be commensurate with the needs of the equipment and the security of access available to the office. Two categories of equipment are addressed in this report:

a. Equipment Requiring A Special Environment.

(1) Criteria. This category refers to equipment which meets one of several of the following criteria:

(a) Equipment requiring a special environment as specified by the manufacturer.

(b) Equipment used to support a sensitive applications.

(c) Equipment serving as a central hub for major processes in support of multiple offices.

(2) Guidelines. If the equipment meets any of the above criteria, then the following guidelines are applicable:

(a) Place equipment in areas that are not

accessible to the public or to unauthorized employees; preferably in a locked room or in a location that is as inconspicuous as possible.

(b) Be sure entrances into rooms or other areas are locked at the end of each workday. Remove keys which provide access and store them in a locked file, desk, or cabinet.

(c) Establish controls to track keys which are assigned to employees who have access to equipment areas.

(d) Store floppy diskettes, disks, and user manuals in a separate, locked cabinet to avoid theft, damage, or accidental destruction.

(e) Place the equipment where it is least likely to sustain damage from leaking of overhead pipes.

(f) Follow the manufacturer's requirements for proper air circulation and/or air conditioning.

(g) Place the equipment near smoke detectors and portable fire extinguishers. If this is not possible, install a smoke detector and portable fire extinguisher next to the equipment.

(h) Maintain a dust-free environment by vacuuming carpeting on a regular basis and/or placing a nonstatic plastic mat under the processor.

(i) Prohibit smoking, eating, and drinking in equipment areas. Post signs to remind employees of these facts.

b. Other Equipment. Physical security for equipment in this category will be dependent on the overall level of physical security for the particular office. That is, if an office is accessible by only APHIS personnel and access is controlled by APHIS personnel, no additional physical security would be required. If the office environment is shared with another Agency or it is a common building and APHIS personnel do not control access, it is likely that additional security measures for the equipment might be necessary. Appropriate judgement should be exercised in determining the additional security measures to be implemented.

4. ADMITTANCE FOR OTHER THAN OFFICIAL BUSINESS

a. Authorized Activities. Agency-occupied space is to be used only for official business and authorized employee activities, including:

(1) Authorized fundraising campaigns, such as the Combined Federal Campaign.

(2) Distribution of circulars or flyers by employee organizations, either in person or through the messenger service or official mail.

(3) Donations by groups of employees for remembrances on special occasions.

b. Unauthorized Activities. Peddling, canvassing, soliciting contributions, distributing unofficial material, and selling insurance, merchandise, or tickets are prohibited in Agency-occupied space.

c. Reporting Unauthorized or Suspicious Persons. Employees should immediately report the presence of unauthorized peddlers, solicitors, or canvassers to the appropriate program official, if located in an Agency-owned or -leased building or the Federal Protective Service, if located in a Federally owned or controlled building.

5. REPORTING THEFTS OR OTHER OFFENSES

a. Reportable offenses include theft of, or damage to, Government-owned or personally owned property or official records; assault; disorderly conduct; or criminally obscene acts which occur in, or on the grounds of, Agency-occupied buildings or space. This includes offenses which occur in Government-controlled or -owned parking areas.

b. Employees should immediately report any of the above offenses to the Designated Official so that the incident can be reported to the proper authorities.

c. The Designated Official should immediately report the offense following the steps shown in Attachment 1.

d. Personally Owned Property Losses are reportable, however, the Agency does not assume responsibility for any loss or damage.

e. Employees who commit any of the offenses stated in paragraph 5.a. are subject to disciplinary action.

/s/ Lonnie J. King

Acting Administrator

PLEASE SEE HARD COPY OR CONTACT MSD, POLICY AND PROGRAM MANAGEMENT BRANCH, THROUGH FTS 2000 ON 301-734-5524 FOR THE PAPER COPY OF ATTACHMENT 1